3GPP TSG SA WG3 Security — S3#16 **S3-000...**

28-30 November, 2000

Sophia Antipolis, France

Title: **LS for "Security risks in introduction phase of MAP security"**

Source: **TSG SA WG3**

To: **TSG SA**

Cc: **TSG CN WG4, GSM association security group**

Contact Person:

Name: Günther Horn

Email: guenther.horn@mchp.siemens.de

Tel : +49 89 636 41494

SA3 are currently working to provide security features to protect MAP signalling messages in the UMTS core network for Release 4 (MAP security). Mechanisms for the management of cryptographic keys to support MAP security are scheduled for Release 5.

At their meeting S3#16 (Sophia, 28-30 Nov, 2000), SA3 discussed security risks during the introduction phase of MAP security. The discussion was based on contribution S3-000688. SA3 came to the conclusion that the introduction of MAP security by a limited number of network operators would give only limited protection even to those network operators who choose to implement MAP security in their networks. The reason for this limited protection is that the networks which implement MAP security would have to continue to exchange MAP messages with other networks with which roaming agreements exist, but which do not implement MAP security. Such MAP messages would necessarily be unprotected. Furthermore, it would not be possible to distinguish between MAP messages truely originating from an unprotected network and MAP messages where the source address was appropriately modified by an attacker.

SA3 consider the stealing of authentication information to be the most critical threat as it could be used by an attacker to impersonate a bona fide subscriber and make calls at his expense, or eavesdrop on the subscriber's calls.

In order to prevent this and other serious threats and provide a meaningful level of protection to network operators in the introduction phase of MAP security SA3 suggest to set a cut-off date for the introduction of MAP security. After this cut-off date, all UMTS operators would have to support MAP protection mode 1 (integrity protection only) as a minimum.

SA3 feel that the GSM association would be the appropriate body to set such a cut-off date.

SA is kindly asked to endorse the proposal by SA3 that a cut-off date for the introduction of MAP security into UMTS networks be set. If SA also feel that the GSM association is the appropriate body to set such a cut-off date SA is kindly asked to send a corresponding LS to the GSM association. It is further suggested that, if SA endorse SA3's proposal, SA3 will directly liaise with the GSM association security group to clarify pertinent technical issues as far as needed.